**Position:** Vice President of the United States

**Institution**: Executive Branch

**Faction:** Political

**Historical Reference:** Joe Biden

**Biography:**

At 66 years old, you have been sworn in as the Vice President of the United States during a period of political transition. Your party has just taken control of both Houses of Congress and the White House. You enter the Administration with decades of legislative and party leadership experience. You are well established in congressional and intelligence circles and enjoy respect from both of the aisles concerning your foreign policy credentials. Both of your presidential campaigns were unsuccessful.

While in the Senate, your primary focus was on foreign policy, criminal justice reform, and drug policy. You twice served as Chair of the prestigious Foreign Relations Committee. You do not have experience with the technical aspects of cybersecurity. While you are not a national security “hawk,” you do believe that the US faces serious security challenges in a globalized system. This includes the possibility that rival governments and non-state actors may use cyber to attack the US from afar. You are entirely loyal to the President. Your goal is for him to be successful.

**Faction Advisory**

Your task is simple, but achieving it is going to be quite complicated. As Vice President, your primary objective here is political. First and foremost, you need a policy that will prevent a large-scale cyber-attack on the US, as this would be politically devastating. In addition, you want to avoid other outcomes that would damage the President politically. This includes ending up in a traditional military conflict that begins in cyber. In addition, this *public* policy, and so it must communicate with things. To the American public, it should signify strength and make citizens feel secure, but it cannot look as if the policy will lead to war. To potential rivals, the NSC policy must send a clear message that cyber-attacks against the US will not be tolerated.

**Assignment**

At an upcoming meeting, the President (instructor) will convene the National Security Council (NSC) and ask it to develop a National Security Strategy for Cyber Security. You need to ensure that the final document the NSC produces reflects your institution’s priorities (see objectives). Because the NSC contains representatives from institutions (or agencies) with vastly different perspectives, this will be no easy task. Government agencies fight hard for influence and resources (e.g., a budget). Not everyone can get what they want. Thus, your colleagues need to hear your ideas, but you also need to convince them that your priorities belong in a document that will not—indeed, *can not*—contain everything. Evidence-based arguments will serve you best here, and you can prepare in the following ways:

* Research your *institution*. What does your institution generally do day-to-day? What are its general interests? This puts you in the mindset of the institution.
* Research the current state of cyberspace (as of January 21, 2009; no later). What are its characteristics? What are its main opportunities and challenges? The instructor will provide you with access to a database of resources to get you started, but you should not confine yourself only to those resources. You may use any time appropriate research.
* Research your policy toward cyberspace. Given (i) and (ii) above, what do you think a national cyber policy needs to contain? What do you think it should avoid? What language should it use?

As the game unfolds, the instructor will distribute additional assignments. You will need to complete those assignments as they arise.

**Objectives**

Your mandate is broad, and there are many different ways that you can ensure that your goals are met. You will need to be both creative and direct in pursuing your agenda. At a minimum, you should seek to:

* A comprehensive policy that addresses all known threats, thereby making the American people feel safer and demonstrating that all aspects of the cybersecurity issue have been addressed.
* A document that makes the President “look good.” - i.e., demonstrates strength, American leadership in the world, and that the public is safe.
* Trade sanctions look good domestically, so whenever possible, this is preferable to military conflict.

You strongly oppose:

* Entrapment. The President needs room to maneuver and to justify US actions. For example, he does not want to be “bogged down” in a war. So you oppose clear “if….then” statements the constrain what the President can do. Think here about creating “political wiggle room” if the US is attacked.
* Excluding any faction’s interests from the final policy

**Strategy Advice**

You will want to encourage the NSC to think about different categories of cyber-attacks, and the different levels of US response that would be appropriate. So, for example, to prevent large-scale “Pearl Harbor” attacks, the US might have to threaten a wide-range of consequences (perhaps), including military action. However, in response to lower-level attacks - intellectual property theft, disinformation campaigns, etc., - may be best deterred with the threat of trade sanctions or “tit-for-tat” American cyber-attacks. Because most of the other factions have narrow interests in cyber, you will need to find a way to convince each side that they are getting some part of what they want. A new global cyber-security agreement would be very beneficial politically because it would demonstrate US global leadership.

Finally, you note that the Bush Administration’s cybersecurity plan emphasized domestic security over a global approach. But the world has changed. You must keep the NSC focused on developing a politically viable strategy that you can “sell” to the American people. This will require compromise among all parties.

**A Cautionary Note**

The game begins on January 21, 2009. Many subsequent administrations, including the current one, likely have a cyberspace policy. Your institution may even currently have cyber-related policies. These, however, will not necessarily be the Administration’s or institution’s *historical*